



MySales

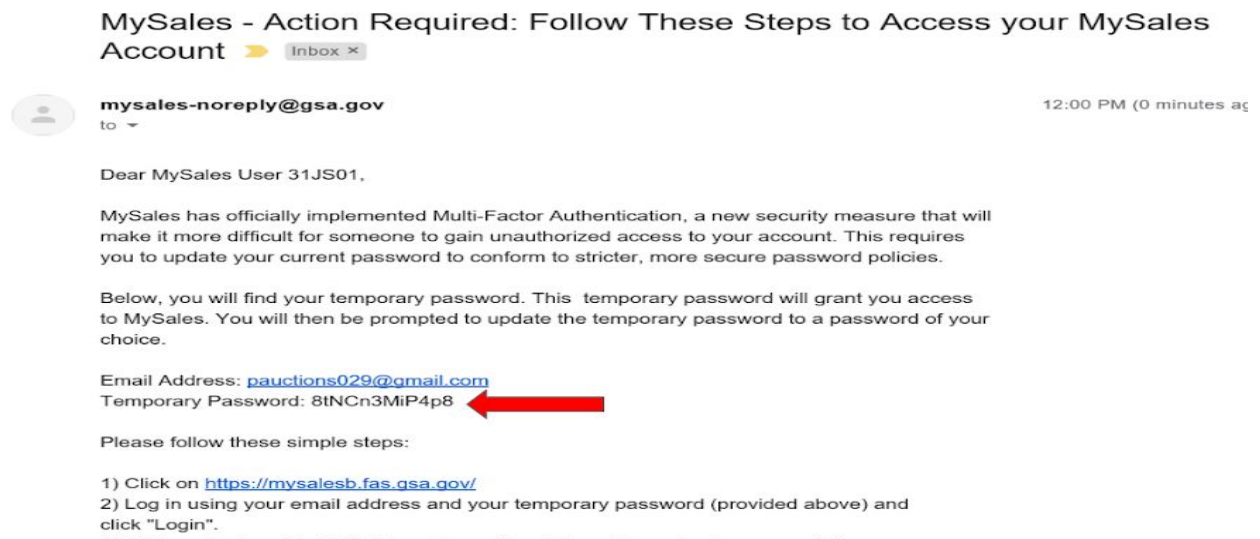
Multi-Factor Authentication (MFA) Help Document

Table of Contents:

How to use your temporary password and set up factors	2
How to set up Email Authentication:	4
How to set up Voice Authentication:	7
How to set up Text (SMS) Authentication:	8
How to set up Google Authenticator:	10
How to log in each day	12
Who should you contact for further help?	15
General FAQs	16

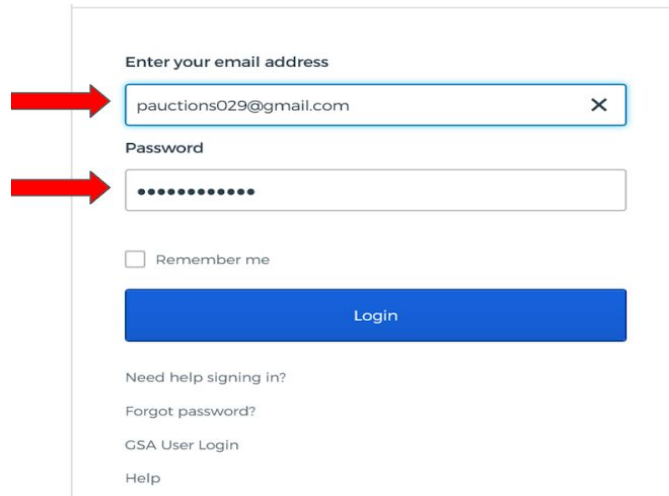
How to use your temporary password and set up factors

Step 1: Check your email. You should have received an email from the MySales system entitled “MySales - Action Required: Follow These Steps to Access your MySales Account.” Copy your temporary password (it will be used on the login screen).



(No email? Please check your spam/junk folder. If you still do not see it, contact the MySales helpdesk at mysales.helpdesk@gsa.gov)

Step 2: Go to <https://mysalesb.fas.gsa.gov/>, and enter in your **email address** and **temporary password** (into the password field). Then, click the “**Login**” button.



Enter your email address

pauctions029@gmail.com X

Password

.....

☐ Remember me

Login

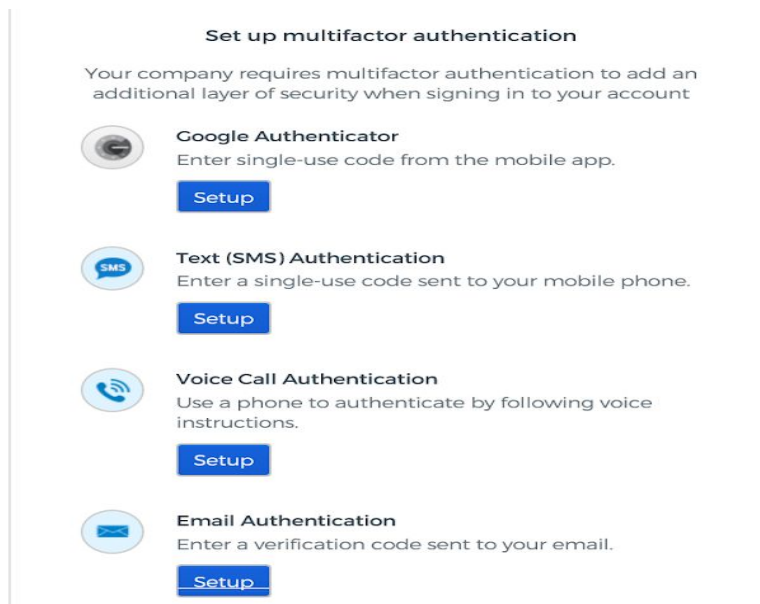
Need help signing in?

Forgot password?

CSA User Login


Help


Step 3: Set up your factors by clicking on “setup” under the Authenticator of your choice. We recommend that you set up at least two factors. (Please note that the email and text authentication is not approved for future use, so please incorporate either voice or Google Authenticator as a factor.)





Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your account

 **Google Authenticator**
Enter single-use code from the mobile app.
[Setup](#)

 **Text (SMS) Authentication**
Enter a single-use code sent to your mobile phone.
[Setup](#)

 **Voice Call Authentication**
Use a phone to authenticate by following voice instructions.
[Setup](#)

 **Email Authentication**
Enter a verification code sent to your email.
[Setup](#)

Step 4: Establish your password. Go back to [step 1](#) and copy your temporary password. Paste your temporary password into the “Current Password” field. Then, create a new password that meets the password requirements.

Password requirements: at least 12 characters, a lowercase letter, an uppercase letter, a number, no parts of your username, does not include your first name, does not include your last name. Your password cannot be any of your last 24 passwords.

Current Password (see help)

.....

New password

.....


Repeat password

.....

Change Password

How to set up Email Authentication:

- 1) Click "Send me the code."



Set up Email Authentication

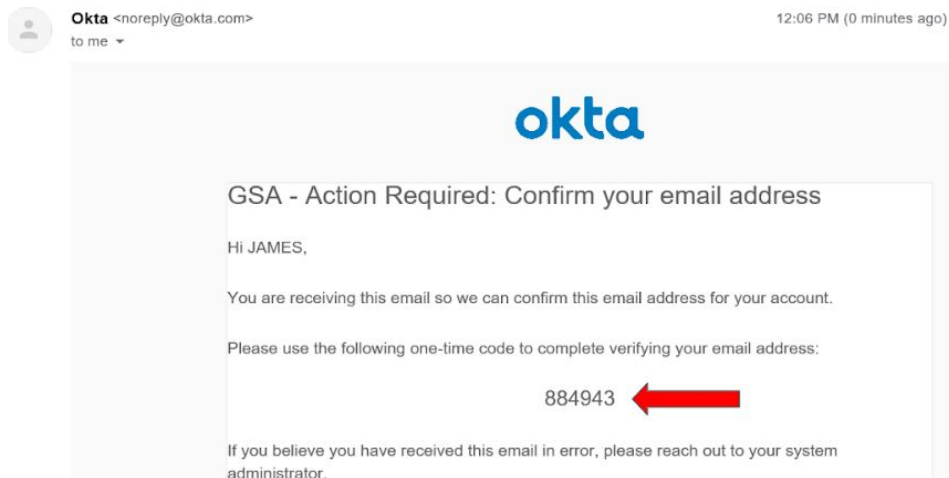
Send a verification code to your registered email.

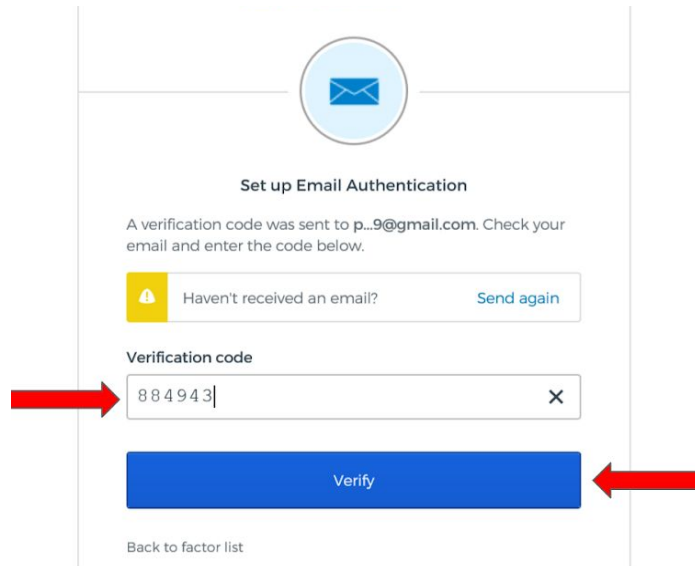
Send me the code


[Back to factor list](#)

- 2) Check your email for an email from OKTA that contains your code. (Please note: If you do not receive an email, check your spam/junk folder. If you still do not see it, please contact the helpdesk.)

3) Enter your code into the field titled “Verification Code,” and then click “Verify.”








Set up Email Authentication

A verification code was sent to p...9@gmail.com. Check your email and enter the code below.

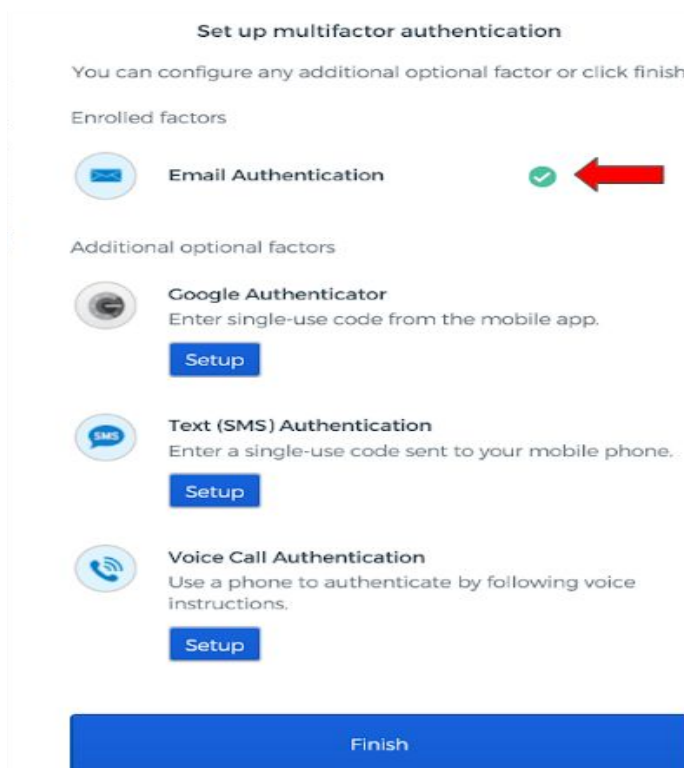
 Haven't received an email? [Send again](#)

Verification code

[Verify](#)

[Back to factor list](#)



- 4) You will see a green checkmark once your email has been successfully set up. (**Please Note:** If you only want to set up one authenticator, you can click “Finish” and you will be taken to step 4.)






Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

-  **Email Authentication**  [Setup](#)

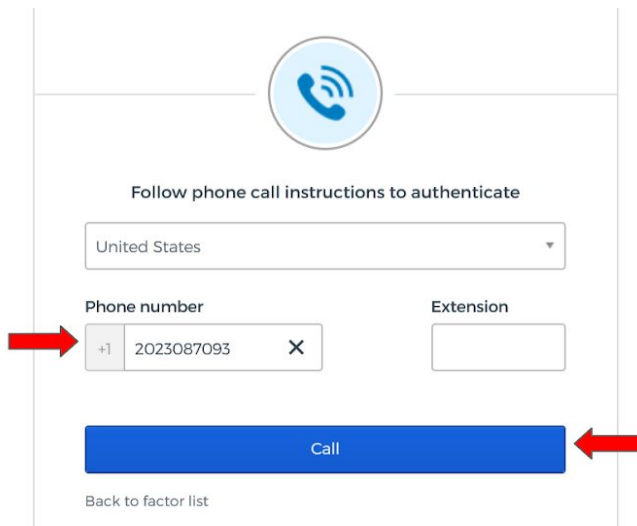
Additional optional factors

-  **Google Authenticator**
Enter single-use code from the mobile app.
[Setup](#)
-  **Text (SMS) Authentication**
Enter a single-use code sent to your mobile phone.
[Setup](#)
-  **Voice Call Authentication**
Use a phone to authenticate by following voice instructions.
[Setup](#)

[Finish](#)

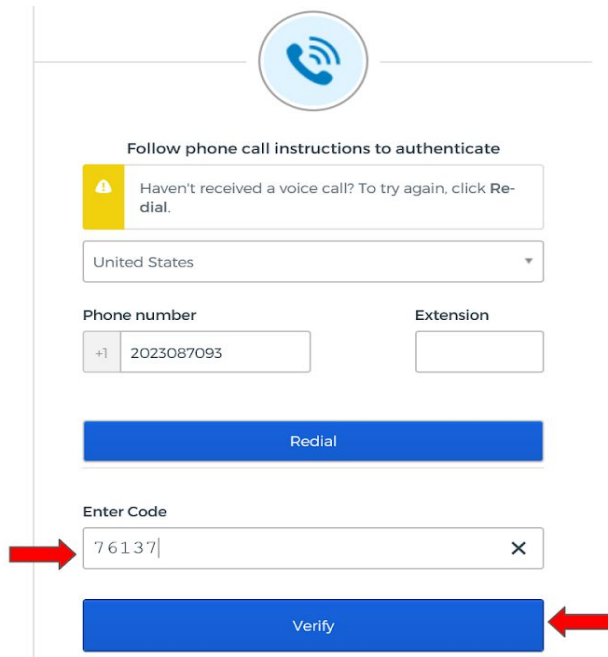
How to set up Voice Authentication:

1. Enter in your phone number (cell or landline), and click “Call.”



This screenshot shows the first step of the voice authentication setup. At the top is a blue phone icon with signal waves. Below it, the text "Follow phone call instructions to authenticate" is centered. A dropdown menu shows "United States". Below that are two input fields: "Phone number" and "Extension". The "Phone number" field contains "+1" in a small box, followed by "2023087093" and a clear 'X' button. A red arrow points to the "+1" box. Below these fields is a large blue button labeled "Call", with a red arrow pointing to it from the right. At the bottom left is a link that says "Back to factor list".

2. You will receive a call with a five digit code. Enter in code and click “Verify.”



This screenshot shows the second step of the voice authentication setup. It features the same blue phone icon at the top. Below the "Follow phone call instructions to authenticate" text is a yellow warning box with a triangle icon and the text: "Haven't received a voice call? To try again, click Redial." Below the warning box is a "United States" dropdown menu. Then are the "Phone number" and "Extension" fields, with the phone number field containing "+1 2023087093". Below these is a blue button labeled "Redial". Further down is an "Enter Code" label above a text input field containing "7 6 1 3 7" with a clear 'X' button. A red arrow points to the input field. At the bottom is a large blue button labeled "Verify", with a red arrow pointing to it from the right.

3. You will see a green checkmark once your voice authentication has been successfully set up. (**Please Note:** If you only want to set up one authenticator, you can click “Finish”

and you will be taken to step 4.)

Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

- Voice Call Authentication**
- Email Authentication**

Additional optional factors

- Google Authenticator**
Enter single-use code from the mobile app.
[Setup](#)
- Text (SMS) Authentication**
Enter a single-use code sent to your mobile phone.
[Setup](#)

[Finish](#)

How to set up Text (SMS) Authentication:

- 1) Enter in your phone number and click “Send Code.” You will receive a six digit code through your mobile device.

Receive a code via Text (SMS) to authenticate

United States

Phone number

[Send code](#)

[Back to factor list](#)

- 2) Enter in your six digit code and click “Verify.”

SMS

Receive a code via Text (SMS) to authenticate

Haven't received an SMS? To try again, click **Re-send code**.

United States

Phone number

+1 2023087093

Re-send code

Enter Code

2 6 8 5 6 2

×

Verify

- 3) You will see a green checkmark once your text (SMS) authentication has been successfully set up. (**Please Note:** If you only want to set up one authenticator, you can click “Finish” and you will be taken to step 4.)

Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

SMS

Text (SMS) Authentication

✓

Voice

Voice Call Authentication

✓

Email

Email Authentication

✓

Additional optional factors

Google Authenticator

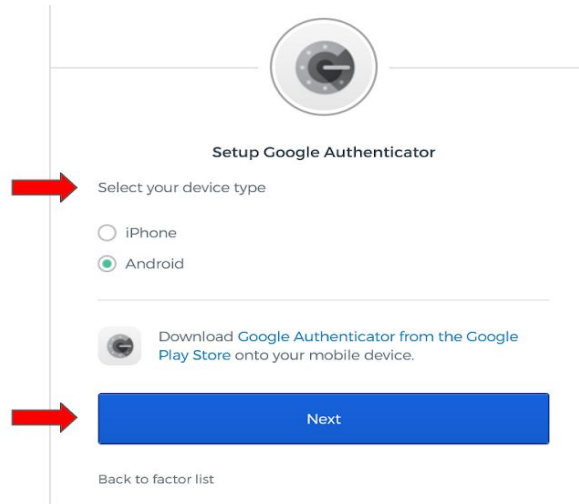
Enter single-use code from the mobile app.

Setup

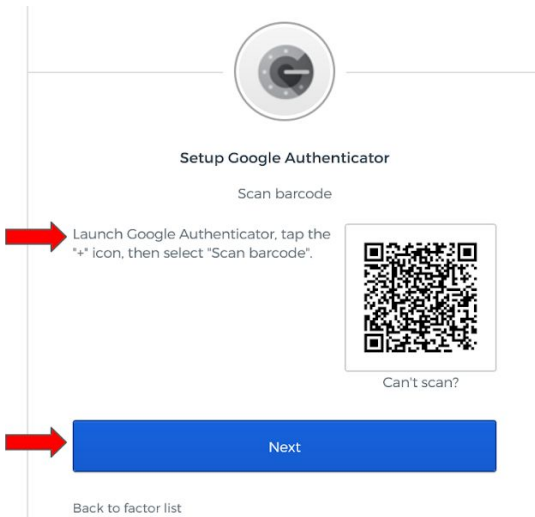
Finish

How to set up Google Authenticator:

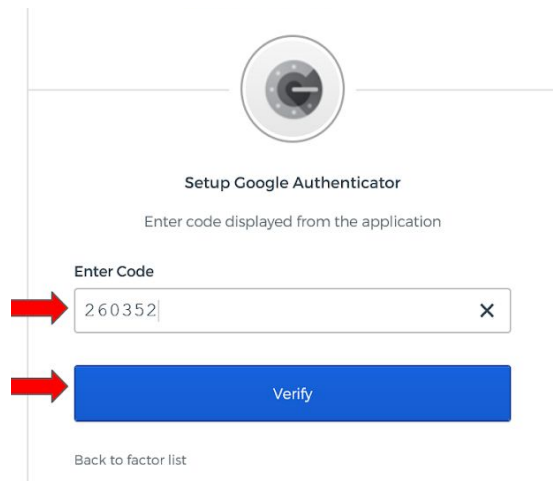
- 1) Open the Google Authentication app on your mobile device.
- 2) Select your device (iPhone or Android) and click "Next."



- 3) From the Google Authenticator app, tap the "+" icon, then select "Scan barcode." Once you scan the barcode, click "Next."



4) Enter in the code generated from the app and then click “Verify.”



Setup Google Authenticator

Enter code displayed from the application

Enter Code

260352

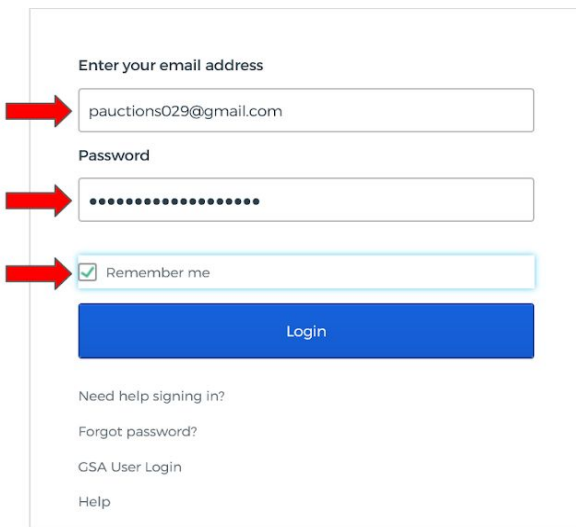
Verify

[Back to factor list](#)

How to log in each day

Step 1: Go to <https://mysales.fas.gsa.gov>, and enter in your **email address** and **new password**. Then, click the “**Login**” button.

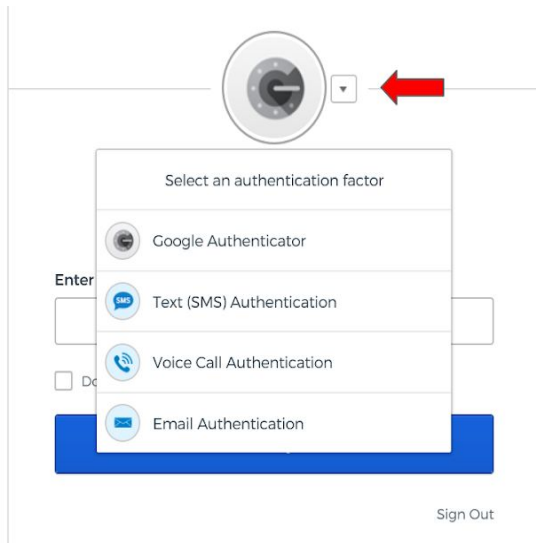
***Important Feature:** By selecting the “Remember me” box at login, the system will pre-populate your email address each time you open the login screen. This prevents you from having to enter it in during each login.



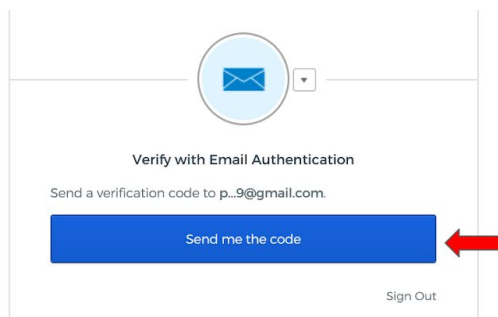
The screenshot shows a login form with the following elements:

- A label "Enter your email address" above a text input field containing "pauctions029@gmail.com". A red arrow points to this field.
- A label "Password" above a password input field filled with dots. A red arrow points to this field.
- A checkbox labeled "Remember me" which is checked. A red arrow points to this checkbox.
- A blue "Login" button.
- Links at the bottom: "Need help signing in?", "Forgot password?", "CSA User Login", and "Help".

Step 2: Select the MFA method that you'd like to use to receive your code. Make sure that you click on the drop down arrow to display all MFA options in case you have set up multiple factors.



Step 3: Go through the process of receiving your code. For the purpose of this example, the code will be emailed. Click on “Send me the code.”

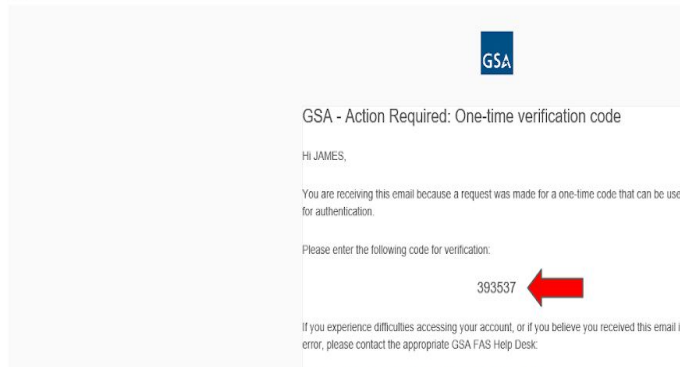


Step 4: Check your email for an email from OKTA. Copy the code from the email and go back to the login page.

Please note: If you do not see the email, please check your junk/spam folder. If you still do not see the code, you can go back to the login screen and click on the “send again” button. If the email still does not come, please contact the helpdesk.

One-time verification code 

Okta <no-reply@okta.com>
to me




Step 5: Enter your code into the field titled “Verification Code,” and then click “Verify.”

***Important Feature:** By selecting the “Do not challenge me on this device for the next 12 hours” you will not be required to submit a one time passcode for 12 hours (assuming you are logging in on the same device as when you selected the option). This option will not display again until the 12 hours have expired. However, if you try logging in from a different device during that 12 hour period, you will be required to request a one time code because the system does not recognize your new device.

Verify with Email Authentication

A verification code was sent to p...9@gmail.com. Check your email and enter the code below.

 Haven't received an email? [Send again](#)

Verification code

☒ Do not challenge me on this device for the next 12 hours

[Verify](#)

[Sign Out](#)

Who should you contact for further help?

Please contact the MySales Helpdesk:

Phone: 1-866-333-7472, Option 4

Email: mysales.helpdesk@gsa.gov

General FAQs

What has changed with login?

Beginning in 2020, GSA Auctions, GSAXcess, Mysales, the NASA Module and the GSA-hosted Computers for Learning website will be making changes to the way you log in.

What will the new login process look like?

- 1) You will log in using your email and password. You will no longer log in using your user ID.
- 2) Every time you log in, a one time code will be sent to the email address listed on your account. You must then enter that code to complete your login.

What is the New Login Process Called?

It is called Multi-Factor Authentication (MFA), and it is an industry standard for both government and private sector websites.

Under MFA, a user is granted access only after presenting two or more pieces of evidence (or factors) to an authentication mechanism. This extra layer of security protects you, GSA, and the government by making it more difficult for someone to gain unauthorized access to your account.

Why do I need to do this?

By preventing unauthorized access to your account, MFA protects you and the Federal Government. It is also a requirement for all Federal Government websites.

Why can't I log in using my user ID?

Your user ID will be tied to your email address. Although you are using your email address to log in, all of your activities will be documented under your unique user ID.

Why do I still need a user ID if I am just going to log in using my email address and password?

You will still have a unique user ID that will be used to formally document all of your activities within the system.

I have multiple accounts with the same email address. How will the system know which account I want to log into?

Once you log into the system with your email address and password, the system will display all available accounts that are linked to your email address. You will have the opportunity to select which account you want to log into.

I use Mysales and GSAXcess. Can I use the same email address and password for both websites?

Assuming your registered email address is the same for both websites, you will be able to use the same email address and password to log into both websites. Once you establish an account by using your email address to log in, you will be able to use that same email address and password for other systems.

What does “Remember me” mean?

By selecting the “Remember me” box at login, the system will pre-populate your email address each time you open the login screen. This prevents you from having to enter it in during each login.

What does “Do not challenge me on this device for the next 12 hours,” mean?

By selecting the “Do not challenge me on this device for the next 12 hours” you will not be required to submit a one time passcode for 12 hours (assuming you are logging in on the same device as when you selected the option). This option will not display again until the 12 hours have expired. However, if you try logging in from a different device during that 12 hour period, you will be required to request a one time code because the system does not recognize your new device.

